(19) **Europäisches Patentamt**

European Patent Office

Office européen des brevets

(11) **EP 0 851 335 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention
of the grant of the patent:
29.10.2003 Bulletin 2003/44

(51) Int Cl.7: **G06F 1/00**

(21) Application number: **97310653.7**

(22) Date of filing: **30.12.1997**

(54) **Secure two-piece user authentication in a computer network**

Gesicherte zweiteilige Benutzer-Authentifizierung in einem Rechnernetz

Authentification en deux pièces sécurisée d'un utilisateur dans un réseau d'ordinateurs

(84) Designated Contracting States:
DE FR GB

(30) Priority: **31.12.1996 US 774809**

(43) Date of publication of application:
01.07.1998 Bulletin 1998/27

(73) Proprietor: **Compaq Computer Corporation**
Houston Texas 77070 (US)

(72) Inventors:
• **Angelo, Michael F.**
  Houston, Texas 77068 (US)
• **Olarig, Sompong P.**
  Cypress, Texas 77429 (US)

(74) Representative: **Brunner, Michael John et al**
GILL JENNINGS & EVERY,
Broadgate House,
7 Eldon Street
London EC2M 7LH (GB)

(56) References cited:
US-A- 5 146 499   US-A- 5 237 614
US-A- 5 497 421   US-A- 5 548 721

• "JEWELRY FOR THE INFORMATION AGE"
ELECTRONICS, vol. 244, no. 17, 18 September
1995, page 49 XP000535371

Description

[0001] The invention relates to security in a computer system, and more particularly to using a cryptographic token to provide two-piece user authentication in a computer network.

[0002] Today's businesses invest large amounts of money in hardware and software, and even more money is spent developing information contained in data files such as text documents and spreadsheets. Protecting such investments can be critical to the success and reputation of a business. Public accounts of the exploits of computer "hackers" -- as malicious code-breakers or eavesdroppers are sometimes called -- have therefore focussed and magnified corporate desires for secure communications and better methods of protecting data. The scope of the problem is undoubtedly even more serious than reported, given the reluctance of many businesses to report security breaches. As a result, security conscious users are requesting that security and integrity features be incorporated into their computer networks to restrict access to data contained on hard drives, as well as information contained in other critical network components.

[0003] One known approach to security involves encryption or cryptography. Cryptography is typically used to protect both data and communications. Generally, an original message or data item is referred to as "plain text", while "encryption" denotes the process of disguising or altering a message in such a way that its substance is not readily discernable. An encrypted message is called "ciphertext". Ciphertext is returned to plain text by an inverse operation referred to as "decryption". Encryption is typically accomplished through the use of a cryptographic algorithm, which is essentially a mathematical function. The most common cryptographic algorithms are key-based, where special knowledge of variable information called a "key" is required to decrypt ciphertext. There are many types of key-based cryptographic algorithms, providing varying levels of security.

[0004] The two most prevalent cryptographic algorithms are generally referred to as "symmetric" (also called secret key or single key algorithms) and "public key" (also called asymmetric algorithms). The security in these algorithms is entered around the keys -- not the details of the algorithm itself. This makes it possible to publish the algorithm for public scrutiny and then mass produce it for incorporation into security products.

[0005] In most symmetric algorithms, the encryption key and the decryption key are the same. This single key encryption arrangement is not flaw-free. The sender and recipient of a message must somehow exchange information regarding the secret key. Each side must trust the other not to disclose the key. Further, the sender must generally communicate the key via another media (similar to a bank sending the personal identification number for an ATM card through the mail). This arrangement is not practical when, for example, the parties interact electronically for the first time over a network. The number of keys also increases rapidly as the number of users increases.

[0006] With public key algorithms, by comparison, the key used for encryption is different from the key used for decryption. It is generally very difficult to calculate the decryption key from an encryption key. In typical operation, the "public key" used for encryption is made public via a readily accessible directory, while the corresponding "private key" used for decryption is known only to the recipient of the ciphertext. In an exemplary public key transaction, a sender retrieves the recipient's public key and uses it to encrypt the message prior to sending it. The recipient then decrypts the message with the corresponding private key. It is also possible to encrypt a message using a private key and decrypt it using a public key. This is sometimes used in digital signatures to authenticate the source of a message.

[0007] One problem with public key algorithms is speed. Public key algorithms are typically on the order of 1,000 times slower than symmetric algorithms. This is one reason that secure communications are often implemented using a hybrid cryptosystem. In such a system, one party encrypts a random "session key" with the other party's public key. The receiving party recovers the session key by decrypting it with his/her private key. All further communications are encrypted using the same session key (which effectively is a secret key) and a symmetric algorithm.

[0008] The number of cryptographic algorithms is constantly growing. The two most popular are DES (Data Encryption Standard) and RSA (named after its inventors --Rivest, Shamir, and Adleman). DES is a symmetric algorithm with a fixed key length of 56 bits. RSA is a public key algorithm that can be used for both encryption and digital signatures. DSA (Digital Signature Algorithm) is another popular public key algorithm that is only used for digital signatures. With any ofthese algorithms, the relative difficulty of breaking an encrypted message by guessing a key with a brute force attack is proportional to the length of the key. For example, if the key is 40 bits long, the total number of possible keys (2^{40}) is about 110 billion. Given the computational power of modern computers, this value is often considered inadequate. By comparison, a key length of 56 bits provides 65,636 times as many possible values as the 40 bit key.

[0009] Much attention has been given to protecting and authenticating communications and data as they are transmitted via internal corporate networks (intranets or LANs) and external networks (such as the Internet). One known method of offering limited access to a networked computer is through the use of passwords. A password is typically stored in a computer's battery-backed CMOS RAM memory. Before the user is allowed access to the computer or secured computer resources, the user is required to enter a password. Once a password is entered, the computer's power-on routine com-

pares the password to the password in CMOS memory and, if they match, the user is allowed access. A main disadvantage of this system is that certain forms of attack can bypass the CMOS memory because in many cases it is not read protected. While generally effective, password protection is one-piece in nature and is only as secure as the password itself.

[0010] Physical keys or tokens, such as those used to unlock a door, have also been used to permit access to a computer system. Like the password approach, this type of security is "one-piece" in nature, and is compromised if the key or token is stolen. Anyone possessing the key can gain access to the computer network and is accorded the same level of access as an authorized user. Currently, there exists no satisfactory method of verifying user identity in granting access privileges in a distributed computing environment.

[0011] US-A-5548721 discloses a method of conducting secure operation in an uncontrolled network in which authorised users are provided with a persona identifier and with a portable, electronically readable card with part of a system key thereon. The system key is created by a secure network access port at the workstation, and, when used in combination with the persona identifier, uniquely identifies the user so that the card and identifier may be used to conduct secure operations from any workstation in the network.

[0012] US-A-5146499 discloses authentication of a smart card utilises a microcomputer provided with an internal leader and an electronic circuit linked to the microcomputer. The circuit includes a microprocessor capable of generating a random factor.

[0013] Briefly, a computer system according to the present invention utilizes a two-piece authentication procedure to securely provide user authentication over a network.

[0014] According to the present invention there is provided a method for securely authenticating user identity in a computer network including a network server coupled to at least one network node capable of communicating with an external token that includes a cryptographic algorithm and an encryption key, the network node further incorporating a secure power-up procedure or other secure operating mode, the method comprising the steps of providing a user password to the network node; communicatively coupling the external token to the network node; providing the user password to the cryptographic algorithm stored in the token; and characterised by: encrypting the user password with the cryptographic algorithm and the encryption key to produce a network password; communicating the network password to the network server; and comparing the network password or portions thereof to information maintained by the network server in order to verify user identity and/or determine network privileges accorded to the network password.

[0015] The method may further comprise the step of enabling or blocking access to a secured network re-

source in response to the result of said step of comparing the network password to information maintained by the network server and this step may comprise utilizing the network password to govern the encryption and decryption of specified data maintained in the network server.

[0016] The step of providing a user password to the network node may be performed while the network node is in a secure period of operation which may include a secure power-up procedure.

[0017] Preferably, prior to the step of communicating the network password to the network server, the method further comprises the step of encrypting the network password using a network public key; and following the step of communicating the network password to the network server, decrypting the network password using a network private key corresponding to the network public key.

[0018] The method may further comprise the step of appending node identification information to the network password prior to communicating the network password to the network server.

[0019] Preferably, the step of comparing the network password or portions thereof to information maintained by the network server includes limiting access to specified data based upon the network password and appended node identification information.

[0020] The step of encrypting the user password with the cryptographic algorithm and the encryption key may occur in the token.

[0021] The step of providing the user password to the cryptographic algorithm may comprise downloading both the cryptographic algorithm and the user password to secure computer memory, and the step of encrypting the user password with the cryptographic algorithm and the encryption key may occur in secure computer memory.

[0022] Preferably, the network password is maintained in secure memory space within the network node.

[0023] The token may be a smart card or a Touch Memory™ device.

[0024] The encryption key may be unique or of limited production.

[0025] Furthermore, according to the present invention there is provided a computer system capable of securely providing two-piece user authentication data over a computer network, the computer system having a secure power-on process or other secure operating mode, the computer system comprising: a system bus; a processor coupled to said system bus; token interface circuitry coupled to said processor for communicating with an external token; network interface circuitry allowing said processor to direct communications to a network server, and characterised by means for operating in conjunction with the external token containing a cryptographic algorithm and an encryption key, and security code stored in a processor readable medium comprising: means for receiving a user password; means for

providing the user password to the external token; means for receiving a network password from the external token, wherein the network password is an encrypted version of the user password; and means for communicating the network password to the network server via said network interface circuitry in order to allow the computer user to access secured network resources.

[0026]   A better understanding of the present invention can be obtained when the following detailed description of the preferred embodiment is considered in conjunction with the following drawings, in which:

Figure 1 is a schematic block diagram of a computer system incorporating capabilities for two-piece user authentication according to the present invention;

Figure 2 is a schematic block diagram of a local area network illustrating secure user authentication and remote peripheral access according to the present invention;

Figure 3 is graphical representation of System Management Mode memory according to the present invention; and

Figures 4A and 4B are flowchart diagrams illustrating a two-piece procedure according to the present invention for entering password information during a secure power-up procedure.

[0027]   The following patents and applications are referenced in the text which follows:

Our US Patent No. 5,537,540, entitled "TRANSPARENT, SECURE COMPUTER VIRUS DETECTION METHOD AND APPARATUS", is hereinafter referred to as the "SAFESTART patent";

Our US Patent No. 5,567,615 entitled, "SECURITY CONTROL FOR A PERSONAL COMPUTER";

Our US Patent No. 5,375,243, entitled "HARD DISK PASSWORD SECURITY SYSTEM";

Our US Patent No. 5,748,888, entitled "METHOD AND APPARATUS FOR PROVIDING SECURE AND PRIVATE KEYBOARD COMMUNICATIONS IN COMPUTER SYSTEMS"; and

Our US Patent No. 5,949,882, entitled "A METHOD AND APPARATUS FOR ALLOWING ACCESS TO SECURED COMPUTER RESOURCES BY UTILIZING A PASSWORD AND EXTERNAL ENCRYPTION ALGORITHM".

[0028]   Referring first to Figure 1, a computer system S according to the present invention is shown. In the preferred embodiment, the system S incorporates two primary buses: a Peripheral Component Interconnect (PCI) bus P which includes an address/data portion and a control signal portion; and an Industry Standard Architecture (ISA) bus I which includes an address portion, a data portion, and a control signal portion. The PCI and ISA buses P and I form the architectural backbone of the computer system S.

[0029]   A CPU/memory subsystem 100 is connected to the PCI bus P. The processor 102 is preferably the Pentium® processor from Intel Corporation, but could be an 80486 or any number of similar or next-generation processors. The processor 102 drives data, address, and control portions 116, 106, and 108 of a host bus HB. A level 2 (L2) or external cache memory 104 is connected to the host bus HB to provide additional caching capabilities that improve the overall performance of the computer system S. The L2 cache 104 may be permanently installed or may be removable if desired. A cache and memory controller 110 and a PCI-ISA bridge chip 130 are connected to the control and address portions 108 and 106 of the host bus HB. The cache and memory controller chip 110 is configured to control a series of data buffers 112. The data buffers 112 are preferably the 82433LX from Intel, and are coupled to and drive the host data bus 116 and a MD or memory data bus 118 that is connected to a memory array 114. A memory address and memory control signal bus is provided from the cache and memory controller 110.

[0030]   The data buffers 112, cache and memory controller 110, and PCI-ISA bridge 130 are all connected to the PCI bus P. The PCI-ISA bridge 130 is used to convert signals between the PCI bus P and the ISA bus I. The PCI-ISA bridge 130 includes: the necessary address and data buffers, arbitration and bus master control logic for the PCI bus P, ISA arbitration circuitry, an ISA bus controller as conventionally used in ISA systems, an IDE (intelligent drive electronics) interface, and a DMA controller. A hard disk drive 140 is connected to the IDE interface of the PCI-ISA bridge 130. Tape drives, CD-ROM devices or other peripheral storage devices (not shown) can be similarly connected.

[0031]   In the disclosed embodiment, the PCI-ISA bridge 130 also includes miscellaneous system logic. This miscellaneous system logic contains counters and activity timers as conventionally present in personal computer systems, an interrupt controller for both the PCI and ISA buses P and I, and power management logic. Additionally, the miscellaneous system logic may include circuitry for a security management system used for password verification and to allow access to protected resources as described more fully below.

[0032]   The PCI-ISA bridge 130 also includes circuitry to generate a "soft" SMI (System Management Interrupt), as well as SMI and keyboard controller interface circuitry. The miscellaneous system logic is connected to the flash ROM 154 through write protection logic 164. Separate enable/interrupt signals are also communicated from the PCI-ISA bridge 130 to the hard drive 140. Preferably, the PCI-ISA bridge 130 is a single integrated circuit, but other combinations are possible.

[0033]   A series of ISA slots 134 are connected to the ISA bus I to receive ISA adapter cards. A series of PCI slots 142 are similarly provided on the PCI bus P to receive PCI adapter cards.

[0034]   A video controller 165 is also connected to the

PCI bus P. Video memory 166 is used to store graphics data and is connected to the video graphics controller 165 and a digital/analog converter (RAMDAC) 168. The video graphics controller 165 controls the operation of the video memory 166, allowing data to be written and retrieved as required. A monitor connector 169 is connected to the RAMDAC 168 for connecting a monitor 170.

[0035] A network interface controller (NIC) 122 is also connected to the PCI bus P, allowing the computer system S to function as a "node" on a network. Preferably, the controller 122 is a single integrated circuit that includes the capabilities necessary to act as a PCI bus master and slave, as well as circuitry required to act as an Ethernet interface. Attachment Unit Interface (AUI) and 10 base-T connectors 124 are provided in the system S, and are connected to the NIC 122 via filter and transformer circuitry 126. This circuitry forms a network or Ethernet connection for connecting the computer system S to a distributed computer environment or local area network (LAN) as shown in Figure 2.

[0036] A combination I/O chip 136 is connected to the ISA bus I. The combination I/O chip 136 preferably includes a real time clock, two UARTS, a floppy disk controller for controlling a floppy disk drive 138, and various address decode logic and security logic to control access to an internal or external CMOS/NVRAM memory (not shown) and stored password values. Further details of contemplated uses of the NVRAM memory are provided below. Additionally, a control line is provided to the read and write protection logic 164 to further control access to the flash ROM 154. Serial port connectors 146 and parallel port connector 132 are also connected to the combination I/O chip 136.

[0037] An 8042, or keyboard controller, is also included in the combination I/O chip 136. The keyboard controller is of conventional design and is connected in turn to a keyboard connector 158 and a mouse or pointing device connector 160. A keyboard 159 is connected to the computer system S through the keyboard connector 158.

[0038] A buffer 144 is connected to the ISA bus I to provide an additional X-bus X for various additional components of the computer system S. A flash ROM 154 receives its control, address and data signals from the X-bus X. Preferably, the flash ROM 154 contains the BIOS information for the computer system and can be reprogrammed to allow for revisions of the BIOS.

[0039] In the disclosed embodiment, the computer system S contains circuitry for communicating with a removable cryptographic token 188. The precise physical nature of the token 188 is not considered critical to the invention. The token can take many forms, such as a Touch Memory™ device supplied by Dallas Semiconductor, Inc., a smart card, or an encryption card. Preferably, the token 188 is easily decoupled from the computer system S and easily transportable by the token bearer. The token 188 contains at least one of a variety of encryption algorithms (such as DES, Blowfish, elliptic curve-based algorithms, etc.). Although the base algorithm can be the same in each token 188, it is preferable that the encryption key be different in each token 188. Ideally, the token 188 is capable of communicating digitally with the computer system S during momentary contact with or proximity to the computer system S. The token 188 of the disclosed embodiment is capable of storing the encryption algorithm in a non-volatile manner and can be permanently write-protected to discourage tampering.

[0040] In the disclosed embodiment of the invention, the circuitry used for establishing a communication link between the token 188 and the computer system S consists of a probe 186 connected to a COM or serial port adapter 184. The port adapter 184 is connected to the RS232 connector 146. Alternatively, the port adaptor 184 could interface with an application specific integrated circuit (ASIC). In operation, the token 188 is detachably received by the probe 186. The probe 186 includes circuitry for reading and writing memory in the token 188, and can be fully powered through the RS232 connector 146. In addition, the probe 186 includes presence detector circuitry for ascertaining the presence of a token 188.

[0041] An additional feature of the computer system S is a System Management Mode (SMM), as discussed at length below in conjunction with Figure 3. It is also noted that Figure 1 presents an exemplary embodiment of the computer system S and it is understood that numerous other effective embodiments could readily be developed as known to those skilled in the art.

[0042] Referring now to Figure 2, a distributed access environment illustrating secure user authentication and remote peripheral access according to the present invention is shown. Two-piece entry of a user password at a network node 200 results in a network password that is securely distributed to over the network to allow access to remote peripherals. In the disclosed embodiment, the secured remote peripheral takes the form of networked hard drives 216, 218 and 220, although access to any secured network resource falls within the scope of the invention.

[0043] The user authentication process occurs similarly in each network node 200, and the description of the process for a single node 200a is provided for sake of clarity. In the disclosed embodiment of the invention, a password entry process is carried out during a secure power-up procedure or other secure mode of operation as detailed more specifically in conjunction with Figures 4A and 4B. During the secure power-up procedure, the computer system S checks for the presence of an external cryptographic token or smart card 188a that is used to store an encryption algorithm furnished with a unique encryption key and optional identification information.

[0044] Following detection of the external token 188a, the computer user is required to enter a plain text user

password. Once entered, the user password is encrypted using an encryption algorithm contained in the external token 188a, thereby generating a "network" password. Alternatively, the external token 188a can generate the network password by performing a one-way hash function on the user password. In either case, the network password is maintained in a secure memory space such as SMM memory 250 (see Figure 3). When the user desires to access a network resource such as a hard drive in a server 201, the network password is appended with an optional session key, the user's public key, or node identification information 204a. The node identification information can be used for a variety of purposes, including limiting access to certain pieces of data to specified users on specified machines. The network password and node information are then encrypted by an encryption algorithm 206a.

[0045] The encryption algorithm 206a can take many forms, including all of the aforementioned algorithms. If a public key/private key algorithm is used, the network server's public key (or any key that is known only to the server) is used with encryption algorithm 206a. The disclosed encryption scheme allows the encrypted network password to be communicated over an unsecured network in such a manner that it is only decipherable by the targeted network server 201.

[0046] Following encryption with the server's public key, the encrypted network password it communicated to the network server 201 via network interface controllers 122a and 122d. The encrypted network password is then decrypted (at element 210) with the server's private key to retrieve the network password. After the network password and any optional session key or node identification information has been decrypted, it is forwarded to a verification process 212 to determine the user's access privileges to hard drives 216, 218, and 220.

[0047] The verification process can take many forms, including an indexed look-up table in which multiple network passwords (in conjunction with any node identification information) are granted the same or a variety of access privileges. Numerous other uses are contemplated for the network password. For example, the password or any appended session keys can be utilized to decrypt or encrypt data on one of the hard drives 216-220 through interface circuitry 214, or as an enablement signal to a password protected device such as the disk drive described in our US-A-5,375,243.

[0048] A one-way hash function or an encryption algorithm can also be used to convert the network password into a pseudo-random seed (intermediate key). The pseudo-random seed could then be used by a deterministic system to generate a public-key/private-key key pair. A common cryptographic algorithm used to generate such keys is DES, but many other algorithms suffice.

[0049] As mentioned, optional keys such as a session key or the user's public key can be appended to the network password prior to its transmission over the network. When an appended session key is provided to the network server 201, subsequent communications between the network node 200a and the network server 201 are encrypted with a symmetric algorithm using the session key. Encryption and decryption with symmetric algorithms is typically much faster than encryption and decryption with public key algorithms.

[0050] Alternatively, the network password could be configured as a subset of a current "super key" by using split key technology. Split key technology refers generally to the process of "splitting" a master key and distributing the portions such that access is contingent upon the presence of different portions. For example, the network server 201 can maintain one piece of the administrative super key and require that a valid network password (the other portion of the split key) be appended before access privileges are granted. The administrative super key can be broken up in different ways, such that multiple network users having different user passwords and unique tokens 188 can access the same secured network resource. The administrative super key can be altered to encompasses additional network passwords as the need arises. Further details of split key technology can be found in US Patent Nos. 5,276,737 and 5,315,658 entitled "FAIR CRYPTOSYSTEMS AND METHODS FOR USE".

[0051] It is also contemplated that the tokens 188 themselves can incorporate identification information in addition to the encryption algorithm, allowing users to have different tokens for different activities -- much like a person having checking and saving accounts that are accessible by the same personal identification number (PIN). Further, the NIC 122a is capable of appending node identification information to the encrypted network password.

[0052] Such uses of the disclosed two-piece user authentication process permit the server hard drives 216-220 or other network resources to be securely compartmentalized with the option to have multiple user levels. This arrangement has many potential applications. For example, a company might not want certain documents to be downloaded outside facility. The invention allows access privileges to be limited to specified nodes 200 within the facility, proving an additional level of security.

The System Management Mode

[0053] Referring now to Figure 3, certain microprocessors, such as the Pentium® processor from Intel Corporation, include a mode referred to as System Management Mode (SMM), which is entered upon receipt of a system management interrupt (SMI). Originally, SMIs were power management interrupts devised by Intel Corporation for portable systems. Portable computers often draw power from batteries which provide a limited amount of energy. To maximize battery life, an SMI is

typically asserted to turn off or reduce the power to any system component that is not currently in use. Although originally meant for laptop computers, SMIs have become popular for desktop and other stationary models as well.

[0054] SMIs are asserted by either an SMI timer, by a system request, or by other means. An SMI is a non-maskable interrupt having almost the highest priority in the system. Only the reset signal R/S* and cache flush signal FLUSH*, which can be conceptualized as interrupts, have a higher priority than the SMI. When an SMI is asserted, a microprocessor maps a portion of memory referred to as SMM memory 250 into the main memory space. The entire CPU state is then saved in the SMM memory 250 (in the CPU register dump 260 of Figure 3) in stack-like, last in/first out fashion. After the initial processor state is saved, the processor 102 begins executing an SMI handler routine 252, which is an interrupt service routine to perform specific system management tasks such as reducing power to specific devices or, as in the case of the present invention, providing security services. While the routine is executed, other interrupt requests are not serviced, and are ignored until the interrupt routine is completed or the microprocessor is reset. When the SMI handler 252 completes its task, the processor state is retrieved from the SMM memory 250, and the main program continues. An SMI active signal referred to as the SMIACT* signal is provided by the processor to indicate operation in SMM.

[0055] As mentioned, following assertion of its SMI input (this is generally an active low signal), the processor 102 calls the SMI handler 252, which addresses an address space that is separate from ordinary main memory. Thereafter, all memory accesses refer only to SMM memory 250. Input/output ("I/O") accesses via instructions such as IN or OUT are still directed to the normal I/O address space, however. One advantageous side-effect of the hardwired separate address SMM area is that the routines stored in this space cannot be snooped by the cache, providing an additional layer of protection.

[0056] In a typical system management mode implementation, it is intended that battery-backed SRAM chips be mapped into the address space between 30000h and 3ffffh by default. External hardware can use the SMIACT* signal as a chip select signal and thereby address either the SRAM chips (the SMIACT* signal is at a logic low level), or the normal main memory (the SMIACT* signal is at a logic high level). By using the SMIACT* signal, then, SMM memory 250 and normal memory can be strictly separated.

[0057] Referring more specifically to Figure 3, a graphical representation of SMM memory 250 as configured according to the present invention is shown. As mentioned above, this address space is addressed by the processor 102 following an SMI. Following an SMI, the state of the processor 102 is stored in the CPU register dump 260. The SMI handler 252 is then called and executed by the processor 102. Importantly, the SMI

handler 252 can be written such that it performs tasks other than power-down operations. An SMI handler 252 written according to the present invention is able to utilize the encrypted user password (network password) 254, encryption keys 256, and an encryption algorithm 258 to securely perform encryption operations that allow a user's identity to be verified over a LAN. Because SMM memory 250 is only addressable while the computer system is in SMM, storing the encrypted user password 254, encryption keys 256 and encryption algorithm 258 in SMM memory 250 prevents malicious code from modifying or reading these sensitive components of the disclosed embodiment of the invention. The optional 32-Kbyte SMM RAM extension 262 can be utilized for securely performing encryption functions or to store additional encryption keys.

[0058] Referring now to Figure 4A and 4B, an exemplary power-on sequence incorporating two-piece user verification according to the invention is shown. The sequence builds upon a secure power-up procedure, such as that described in the SAFESTART patent. Briefly, this invention reduces the administrative requirements of earlier secure power-on techniques. A reserved non-DOS hard disk partition is used to pre-boot the computer system S and provide a secure environment from which to verify files. Upon power-up or reset, the computer performs the power-on self test (POST), during which it checks a SAFESTART track by comparing its hash value to a value stored in NVRAM. If the integrity of the SAFESTART track is verified, the first "SAFESTART" routine is loaded into memory and executed.

[0059] The SAFESTART routine first checks the master boot record and boot sectors of the hard disk. This verification captures a large majority of viruses and is performed before any code residing in those areas is executed, thus preventing the spread of any discovered viruses. Further checks are performed on SAFESTART files before each is executed. Eventually, system files and any additional designated user files are verified. Since the computer system was booted from an atypical partition, the drives are remapped to account for the shift in logical disk drive addressing. When the verification process is completed, SAFESTART files are cleaned up, a latch is set to prevent unauthorized modification of the initial hash values, and control is returned to the BIOS to boot the user operating system. Thus, a computer system implemented according to the SAFESTART patent insures that designated software and passwords are trustworthy following a power-up cycle.

[0060] As shown in Figure 2A, when power to the computer system S is initially applied or the system undergoes a cold restart, the POWER-ON sequence 300 is commenced. In the first step 302 of the POWER-ON sequence 200 the computer system S begins executing from BIOS ROM. The BIOS is preferably stored in flash ROM 154 and contains low level programming for booting the operating system, and an interrupt handler for accessing the hard drive 140. Control then proceeds to

step 304 where the computer system S performs a power-on self test (POST) to determine if all system hardware is operating properly.

[0061]   Following additional power-on steps (optional), control next proceeds to step 306 for commencement of a secure power-up procedure such as that described in the SAFESTART patent. In the preferred embodiment, operating sequences for the secure power-up procedure are configured as an option ROM and located in the option ROM address space in a conventional manner. Preferably, the operating sequences are provided as the last option ROM in order to allow any other option ROM's to be installed at the outset. The system BIOS executes this portion of the secure power-on sequence as a part of its scan for option ROMs, which are executed when encountered in POST. This arrangement requires address decoding for the power-on sequence, but also simplifies distribution into a family of computer systems. Alternatively, the power-on sequence could be implemented as a direct call from the BIOS, rather than an option ROM call.

[0062]   Control next proceeds to step 308 to determine if a token 188 containing an encryption algorithm is present. If the aforementioned presence detection circuitry determines that a token is not present, control loops to step 310 to display a message requesting that the user provide a token 188. When a token 188 is present as determined in step 308, control passes to step 312 where the user is prompted to enter a plain text user password. As an alternative to a memorized value, the plain text password could be generated with the aid of biometrics. For example, a scanned fingerprint could be converted into a plain text password value. It is noted that the precise ordering of steps 308-312 is not considered critical to the invention.

[0063]   Control next proceeds to step 314 of Figure 4B and the user password is encrypted using the encryption algorithm provided by the external token 188. The encrypted plain text password effectively becomes the network password. The encryption algorithm that is utilized by the token 188 can take many forms, including DES, RSA, DSA, RC2, RC4, Blowfish, IDEA, 3-WAY, and MDC among others. Ideally, the algorithm in each token 188 is enabled by an encryption key that is unique or of limited production, such that it is impractical or impossible to circumvent the verification process by using a substitute token.

[0064]   It is contemplated that the actual encryption process could be carried out by the token 188 itself. In this embodiment of the invention, the user password is transmitted to the token 188 through the RS232 connector 146 or alternate connection port. The token 188 then performs the encryption function using its stored encryption algorithm and associated encryption key. Following the encryption process, the encrypted password is returned to the computer system S via the RS232 connector 146.

[0065]   In an alternate embodiment of the invention,

the encryption algorithm is downloaded into computer memory. After the user password has been entered, the encryption function is then performed by the computer system S. In this embodiment of the invention, it is desirable that the encryption algorithm be erased from the computer memory after completion of the encryption process and while the computer system S is still in the secure power-on period. This step prevents the encryption algorithm from being surreptitiously obtained from memory following the secure power-on period.

[0066]   Following creation of the network password, control proceeds to step 316 and optional node identification information (or a session key) is appended. As mentioned above, node identification information allows the network server 201 to determine which node is being utilized and grant access privileges accordingly. The optional node identification information can be appended prior to the encryption process of step 314. In either case, control next proceeds to step 318 and the network password and any appended node identification information are stored in secure memory such as SMM memory 250. The network password could also be maintained in protected/locked NVRAM or Flash ROM 154, or in some other secure memory such as that disclosed in the previously referenced US patent application serial no. 08/396343. Following this step, control proceeds to step 320 and the secure power-up procedure is continued.

[0067]   It should be observed that in each of the embodiments of the invention described above, the user authentication or password verification process is two-piece in nature. If either the user password or the external token is misappropriated, it is of little value. Both pieces are required to generate the network password. In addition, the scope of the invention not considered to be limited to the disclosed secure power-up procedure. Likewise, the precise ordering of the power-up steps is not considered critical to the invention.

[0068]   In one alternate embodiment of the invention, the two-piece authentication process is conducted during normal computer operation outside of the secure power-on sequence. In this embodiment of the invention, the user password is communicated to secure memory by means of a secure keyboard communications channel such as that described in previously referenced US patent application no. 08/657982. Briefly, a request for secure keyboard communications causes the computer's processor to enter into SMM. The SMI handler then directs specialized hardware to intercept and divert keyboard interrupts, such that data entered via the keyboard is only communicated to secure, non-readable memory. The secured keyboard communications channel prevents the user's plain text password from being intercepted by malicious software code, such as a virus masquerading as a screen saver or device driver.

[0069]   Thus, a method has been described for permitting secure user authentication and remote peripheral

access based upon a two-piece user verification process. In the disclosed embodiment of the invention, the user verification process begins during a secure power-up procedure. At some point during the secure power-up procedure, the computer user is required to provide an external token or smart card. The token or smart card is used to store an encryption algorithm furnished with an encryption key that is unique or of limited production. The computer user is then required to enter a plain text user password. Once entered, the user password is encrypted using the encryption algorithm contained in the external token to create a network password. When the network user desires to access a secured network resource, the network password is then encrypted using the network server's public key before being communicated over the network. Once received by the server, the encrypted network password is decrypted using the server's public key. A user verification process is then performed on the network password to determine which, if any, access privileges have been accorded the network user. Optional node identification information can be appended to the network password to provide additional levels of access. The two-piece nature of the authentication process assures that if either the user password or the external token is stolen, it is of little value. Both pieces are required to access protected resources and uniquely identify a user to the network.

Claims

1. A method for securely authenticating user identity in a computer network including a network server (201) coupled to at least one network node (200a) capable of communicating with an external token (188) that includes a cryptographic algorithm and an encryption key (256), the network node (200a) further incorporating a secure power-up procedure or other secure operating mode, the method comprising the steps of:

   providing a user password to the network node (200a);
   communicatively coupling the external token (188) to the network node (200a);
   providing the user password to the cryptographic algorithm stored in the token (188); and
   characterised by:

   encrypting the user password with the cryptographic algorithm and the encryption key (256) to produce a network password (254);
   communicating the network password (254) to the network server (201); and
   comparing the network password (254) or portions thereof to information maintained by the network server (201) in order to ver-

ify user identity and/or determine network privileges accorded to the network password (254).

2. The method of claim 1, further comprising the step of:

   enabling or blocking access to a secured network resource (216,218,220) in response to the result of said step of comparing the network password (254) to information maintained by the network server (201).

3. The method of claim 1, wherein said step of enabling or blocking access to a secured network resource (216,218,220) comprises utilizing the network password (254) to govern the encryption and decryption of specified data maintained in the network server (201).

4. The method of claim 1, wherein said step of providing a user password to the network node (200a) is performed while the network node (200a) is in a secure period of operation.

5. The method of claim 4, wherein the secure period of operation includes a secure power-up procedure.

6. The method of claim 1, further comprising the steps of:

   prior to said step of communicating the network password (254) to the network server (201), encrypting the network password (254) using a network public key (206a); and
   following said step of communicating the network password (254) to the network server (201), decrypting the network password (254) using a network private key (210) corresponding to the network public key (206a).

7. The method of claim 1, further comprising the step of appending node identification information (204a) to the network password (254) prior to communicating the network password (254) to the network server (201).

8. The method of claim 7, wherein said step of comparing the network password (254) or portions thereof to information maintained by the network server (201) includes limiting access to specified data based upon the network password (254) and appended node identification information (204a).

9. The method of claim 1, wherein said step of encrypting the user password with the cryptographic algorithm and the encryption key (256) occurs in the token (188).

10. The method of claim 1, wherein said step of providing the user password to the cryptographic algorithm comprises downloading both the cryptographic algorithm and the user password to secure computer memory, and wherein said step of encrypting the user password with the cryptographic algorithm and the encryption key (256) occurs in secure computer memory.

11. The method of claim 1, wherein the network password (254) is maintained in secure memory space (SMM) within the network node (200a).

12. The method of claim 1, wherein the token (188) is a smart card.

13. The method of claim 1, wherein the token (188) is a Touch Memory™ device.

14. The method of claim 1, wherein the encryption key (256) is unique or of limited production.

15. A computer system (S) capable of securely providing two-piece user authentication data over a computer network, the computer system (S) having a secure power-on process or other secure operating mode, the computer system (S) comprising:

    a system bus (HB);
    a processor (102) coupled to said system bus (HB);
    token interface circuitry coupled to said processor (102) for communicating with an external token (188);
    network interface circuitry allowing said processor (102) to direct communications to a network server (201); and **characterised by**
    means for operating in conjunction with the external token (188) containing a cryptographic algorithm and an encryption key (256), and security code stored in a processor readable medium comprising:

        means for receiving a user password;
        means for providing the user password to the external token (188);
        means for receiving a network password (254) from the external token (188), wherein the network password (254) is the user password encrypted with said cryptographic algorithm and said encryption key (256); and
        means for communicating the network password (254) to the network server (201) via said network interface circuitry in order to allow the computer user to access secured network resources (216,218,220).

16. The computer system (S) of claim 15, wherein said security code is executed while the computer system (S) is in a secure operating mode.

17. The computer system (S) of claim 15, wherein said secure operating mode is a secure power-on procedure.

18. The computer system (S) of claim 15, wherein said security code further causes said processor to encrypt the network password using the network server's public key prior to said step of communicating the network password to the network server.

19. The computer system (S) of claim 15, wherein said security code further causes said processor (102) to append node identification information (204a) to the network password (254) prior to said step of communicating the network password (254) to the network server (201).

20. The computer system (S) of claim 15, wherein the external token (188) is a smart card.

21. The computer system (S) of claim 15, wherein the external token (188) is a Touch Memory™ device.

22. The computer system (S) of claim 15, wherein the encryption key (256) is unique or of limited production.

Patentansprüche

1. Verfahren zur gesicherten Authentifizierung der Benutzeridentität in einem Rechnernetz, das einen Netzwerk-Server (201) umfasst, der mit wenigstens einem Netzwerkknoten (200a) gekoppelt ist und in der Lage ist, mit einem äußeren Token (188) zu kommunizieren, das einen kryptografischen Algorithmus und einen Verschlüsselungsschlüssel (256) umfasst, wobei der Netzwerkknoten (200a) außerdem eine sichere Hochfahrprozedur oder einen sonstigen sicheren Betriebsmodus umfasst, wobei das Verfahren folgende Schritte umfasst:

-    Bereitstellen eines Benutzerpasswortes für den Netzwerkknoten (200a);

-    kommunikatives Koppeln des äußeren Tokens (188) mit dem Netzwerkknoten (200a);

-    Bereitstellen des Benutzerpasswortes für den in dem Token (188) gespeicherten kryptografischen Algorithmus; und **gekennzeichnet durch**

-    Verschlüsseln des Benutzerpasswortes mit

dem kryptografischen Algorithmus und dem Verschlüsselungsschlüssel (256), um ein Netzwerkpasswort (254) zu erzeugen;

- Weitergeben des Netzwerkpasswortes (254) an den Netzwerk-Server (201); und

- Vergleichen des Netzwerkpasswortes (254) oder von Teilen davon mit den von dem Netzwerk-Server (201) verwalteten Informationen, um die Benutzeridentität zu überprüfen bzw. dem Netzwerkpasswort (254) gewährte Netzwerkprivilegien zu bestimmen.

2. Verfahren nach Anspruch 1, zusätzlich folgenden Schritt umfassend:

- Ermöglichen oder Blockieren des Zugriffs auf eine gesicherte Netzwerkausstattung (216, 218, 220) als Reaktion auf das Ergebnis aus dem Schritt des Vergleichens des Netzwerkpasswortes (254) mit den von dem Netzwerk-Server (201) verwalteten Informationen.

3. Verfahren nach Anspruch 1, wobei der Schritt, den Zugriff auf eine gesicherte Netzwerkausstattung (216, 218, 220) zu ermöglichen oder zu blockieren, das Verwenden des Netzwerkpasswortes (254) umfasst, um die Verschlüsselung und Entschlüsselung von spezifizierten Daten zu regeln, die von dem Netzwerk-Server (201) verwaltet werden.

4. Verfahren nach Anspruch 1, wobei der Schritt, ein Benutzerpasswort für den Netzwerkknoten (200a) bereitzustellen, durchgeführt wird, während sich der Netzwerkknoten (200a) in einem sicheren Betriebszeitraum befindet.

5. Verfahren nach Anspruch 4, wobei der sichere Betriebszeitraum eine sichere Hochfahrprozedur umfasst.

6. Verfahren nach Anspruch 1, zusätzlich folgende Schritte umfassend:

- vor dem Schritt des Weitergebens des Netzwerkpasswortes (254) an den Netzwerk-Server (201) Verschlüsseln des Netzwerkpasswortes (254) unter Verwendung eines öffentlichen Netzwerkschlüssels (206a); und

- nach dem Schritt des Weitergebens des Netzwerkpasswortes (254) an den Netzwerk-Server (201) Entschlüsseln des Netzwerkpasswortes (254) unter Verwendung eines dem öffentlichen Netzwerkschlüssel (206a) entsprechenden privaten Netzwerkschlüssels (210).

7. Verfahren nach Anspruch 1, das zusätzlich den Schritt des Anhängens von Knotenidentifizierungsinformationen (204a) an das Netzwerkpasswort (254) umfasst, bevor das Netzwerkpasswort (254) an den Netzwerk-Server (201) weitergegeben wird.

8. Verfahren nach Anspruch 7, wobei der Schritt, bei dem das Netzwerkpasswort (254) oder Teile davon mit von dem Netzwerk-Server (201) verwalteten Informationen verglichen werden, das Beschränken des Zugriffs auf spezifizierte Daten anhand des Netzwerkpasswortes (254) und von Knotenidentifizierungsinformationen (204a) umfasst.

9. Verfahren nach Anspruch 1, wobei der Schritt des Verschlüsselns des Benutzerpasswortes mit dem kryptografischen Algorithmus und dem Verschlüsselungsschlüssel (256) in dem Token (188) geschieht.

10. Verfahren nach Anspruch 1, wobei der Schritt, bei dem das Benutzerpasswort für den kryptografischen Algorithmus bereitgestellt wird, das Herunterladen sowohl des kryptografischen Algorithmus als auch des Benutzerpasswortes in sicheren Rechnerspeicher umfasst und der Schritt des Verschlüsselns des Benutzerpasswortes mit dem kryptografischen Algorithmus und dem Verschlüsselungsschlüssel (256) in sicherem Rechnerspeicher geschieht.

11. Verfahren nach Anspruch 1, wobei das Netzwerkpasswort (254) auf sicherem Speicherplatz (SMM) innerhalb des Netzwerkknotens (200a) verwaltet wird.

12. Verfahren nach Anspruch 1, wobei das Token (188) eine intelligente Chip-Karte ist.

13. Verfahren nach Anspruch 1, wobei das Token (188) eine Touch Memory™-Vorrichtung ist.

14. Verfahren nach Anspruch 1, wobei der Verschlüsselungsschlüssel (256) eindeutig oder von beschränkter Erzeugung ist.

15. Rechnersystem (S), das in der Lage ist, gesichert zweiteilige Benutzer-Authentifizierungsdaten über ein Rechnernetzwerk bereitzustellen, wobei das Rechnersystem (S) einen sicheren Einschaltprozess oder einen sonstigen Betriebsmodus aufweist und das Rechnersystem (S) Folgendes umfasst:

- einen Systembus (HB);

- einen mit dem Systembus (HB) gekoppelten Prozessor (102);

- eine mit dem Prozessor (102) gekoppelte To-ken-Schnittstellenschaltung zum Kommunizie-ren mit einem äußeren Token (188);

- Netzwerkschnittstellenschaltung, die es dem Prozessor (102) ermöglicht, Mitteilungen an ei-nen Netzwerk-Server (201) zu richten; und **ge-kennzeichnet durch**

- Einrichtungen zum Betrieb in Verbindung mit dem äußeren Token (188), das einen krypto-grafischen Algorithmus und einen Verschlüsse-lungsschlüssel (256) umfasst; und

- Sicherheitscode, der in einem von einem Pro-zessor lesbaren Medium gespeichert ist, um-fassend:

  - Einrichtungen zum Empfangen eines Be-nutzerpasswortes;

  - Einrichtungen zum Bereitstellen des Be-nutzerpasswortes für das äußere Token (188);

  - Einrichtungen zum Empfangen des Netz-werkpasswortes (254) von dem äußeren Token (188), wobei das Netzwerkpasswort (254) das mit dem kryptografischen Algo-rithmus und dem Verschlüsselungsschlüs-sel (256) verschlüsselte Benutzerpasswort ist; und

  - Einrichtungen zum Weitergeben des Netz-werkpasswortes (254) an den Netzwerk-Server (201) über die Netzwerkschnittstel-lenschaltung, um dem Rechnerbenutzer den Zugriff auf gesicherte Netzwerkaus-stattungen (216, 218, 220) zu ermöglichen.

16. Rechnersystem (S) nach Anspruch 15, wobei der Sicherheitscode ausgeführt wird, während sich das Rechnersystem (S) in einem sicheren Betriebsmo-dus befindet.

17. Rechnersystem (S) nach Anspruch 15, wobei der sichere Betriebsmodus eine sichere Einschalt-prozedur ist.

18. Rechnersystem (S) nach Anspruch 15, wobei der Sicherheitscode außerdem den Prozessor veran-lasst, vor dem Schritt des Weitergebens des Netz-werkpasswortes an den Netzwerk-Server das Netz-werkpasswort unter Verwendung des öffentlichen Schlüssels des Netzwerks zu verschlüsseln.

19. Rechnersystem (S) nach Anspruch 15, wobei der Sicherheitscode außerdem den Prozessor (102)

veranlasst, vor dem Schritt des Weitergebens des Netzwerkpasswortes (254) an den Netzwerk-Ser-ver (201) Knotenidentifizierungsinformationen (204a) an das Netzwerkpasswort (254) anzuhän-gen.

20. Rechnersystem (S) nach Anspruch 15, wobei das Token (188) eine intelligente Chip-Karte ist.

21. Rechnersystem (S) nach Anspruch 15, wobei das Token (188) eine Touch Memory™-Vorrichtung ist.

22. Rechnersystem (S) nach Anspruch 15, wobei der Verschlüsselungsschlüssel (256) eindeutig oder von beschränkter Erzeugung ist.

Revendications

1. Un procédé pour authentifier de manière sûre une identité d'utilisateur dans un réseau informatique in-cluant un serveur de réseau (201) couplé à au moins un noeud de réseau (200a) capable de com-muniquer avec un jeton externe (188) qui comporte un algorithme cryptographique et une clé de chiffre-ment (256), le noeud de réseau (200a) comportant en outre une procédure de mise sous tension sécu-risée ou un autre mode de fonctionnement sécuri-sé, le procédé comprenant les étapes suivantes :

    on fournit un mot de passe d'utilisateur au noeud de réseau (200a);
    on couple pour la communication le jeton ex-terne (188) au noeud de réseau (200a);
    on fournit le mot de passe d'utilisateur à l'algo-rithme cryptographique stocké dans le jeton (188); et **caractérisé par** les étapes suivantes:

        on chiffre le mot de passe d'utilisateur avec l'algorithme cryptographique et la clé de chiffrement (256) pour produire un mot de passe de réseau (254);
        on communique le mot de passe de réseau (254) à un serveur de réseau (201); et
        on compare le mot de passe de réseau (254) ou des parties de celui-ci avec une information conservée par le serveur de ré-seau (201), afin de vérifier l'identité de l'uti-lisateur et/ou de déterminer des privilèges de réseau accordés au mot de passe de réseau (254).

2. Le procédé selon la revendication 1, comprenant en outre l'étape suivante :

    on accorde ou on bloque l'accès à une ressour-ce de réseau sécurisée (216, 218, 220) en ré-ponse au résultat de l'étape de comparaison du

mot de passe de réseau (254) avec de l'information conservée par le serveur de réseau (201).

3. Le procédé selon la revendication 1, dans lequel l'étape d'accord ou de blocage de l'accès à une ressource de réseau sécurisée (216, 218, 220) comprend l'utilisation du mot de passe de réseau (254) pour piloter le chiffrement et le déchiffrement de données spécifiées conservées dans le serveur de réseau (201).

4. Le procédé selon la revendication 1, dans lequel l'étape de fourniture d'un mot de passe d'utilisateur au noeud de réseau (200a) est accomplie pendant que le noeud de réseau (200a) est dans une période de fonctionnement sécurisée.

5. Le procédé selon la revendication 4, dans lequel la période de fonctionnement sécurisée comprend une procédure de mise sous tension sécurisée.

6. Le procédé selon la revendication 1, comprenant en outre les étapes suivantes :

avant l'étape de communication du mot de passe de réseau (254) au serveur de réseau (201), on chiffre le mot de passe de réseau (254) en utilisant une clé publique de réseau (206a); et à la suite de l'étape de communication du mot de passe de réseau (254) au serveur de réseau (201), on déchiffre le mot de passe de réseau (254) en utilisant une clé privée de réseau (210) correspondant à la clé publique de réseau (206a).

7. Le procédé selon la revendication 1, comprenant en outre l'étape consistant à annexer une information d'identification de noeud (204a) au mot de passe de réseau (254) avant de communiquer le mot de passe de réseau (254) au serveur de réseau (201).

8. Le procédé selon la revendication 7, dans lequel l'étape de comparaison du mot de passe de réseau (254) ou de parties de celui-ci avec une information conservée par le serveur de réseau (201) comprend la limitation de l'accès à des données spécifiées, sur la base du mot de passe de réseau (254) et de l'information d'identification de noeud (204a) annexée.

9. Le procédé selon la revendication 1, dans lequel l'étape de chiffrement du mot de passe d'utilisateur avec l'algorithme cryptographique et la clé de chiffrement (256) a lieu dans le jeton (188).

10. Le procédé selon la revendication 1, dans lequel

l'étape consistant à fournir le mot de passe d'utilisateur à l'algorithme cryptographique comprend le téléchargement à la fois de l'algorithme cryptographique et du mot de passe d'utilisateur vers une mémoire d'ordinateur sécurisée, et dans lequel l'étape de chiffrement du mot de passe d'utilisateur avec l'algorithme cryptographique et la clé de chiffrement (256) a lieu dans la mémoire d'ordinateur sécurisée.

11. Le procédé selon la revendication 1, dans lequel le mot de passe de réseau (254) est conservé dans un espace de mémoire sécurisé (SMM) à l'intérieur du noeud de réseau (200a).

12. Le procédé selon la revendication 1, dans lequel le jeton (188) est une carte à microprocesseur.

13. Le procédé selon la revendication 1, dans lequel le jeton (188) est un dispositif Touch Memory (marque déposée).

14. Le procédé selon la revendication 1, dans lequel la clé de chiffrement (256) est unique ou produite en quantité limitée.

15. Un système d'ordinateur (S) capable de fournir manière sûre des données d'authentification d'utilisateur en deux parties, sur un réseau informatique, le système d'ordinateur (S) ayant un processus de mise sous tension sécurisé ou un autre mode de fonctionnement sécurisé, le système d'ordinateur (S) comprenant :

un bus de système (HB);
un processeur (102) couplé au bus de système (HB);
un circuit d'interface de jeton couplé au processeur (102) pour communiquer avec un jeton externe (188);
un circuit d'interface de réseau permettant au processeur (102) de diriger des communications vers un serveur de réseau (201); et **caractérisé par**
un moyen prévu pour fonctionner en association avec le jeton externe (188), contenant un algorithme cryptographique et une clé de chiffrement (256), et
un code de sécurité stocké sur un support lisible par processeur, comprenant :

un moyen pour recevoir un mot de passe d'utilisateur;
un moyen pour fournir le mot de passe d'utilisateur au jeton externe (188)
un moyen pour recevoir un mot de passe de réseau (254) provenant du jeton externe (188), le mot de passe de réseau (254) étant chiffré avec l'algorithme cryptogra-

phique et la clé de chiffrement (256); et
un moyen pour communiquer le mot de
passe de réseau (254) au serveur de ré-
seau (201) par l'intermédiaire du circuit
d'interface de réseau, afin de permettre à
l'utilisateur de l'ordinateur d'accéder à des
ressources de réseau sécurisées (216,
218, 220).

16. Le système d'ordinateur (S) selon la revendication
15, dans lequel le code de sécurité est exécuté pen-
dant que le système d'ordinateur (S) est dans un
mode de fonctionnement sécurisé.

17. Le système d'ordinateur (S) selon la revendication
15, dans lequel le mode de fonctionnement sécuri-
sé est une procédure de mise sous tension sécuri-
sée.

18. Le système d'ordinateur (S) selon la revendication
15, dans lequel le code de sécurité commande en
outre au processeur de chiffrer le mot de passe de
réseau en utilisant la clé publique du serveur de ré-
seau, avant l'étape de communication du mot de
passe de réseau au serveur de réseau.

19. Le système d'ordinateur (S) de la revendication 15,
dans lequel le code de sécurité commande en outre
au processeur (102) d'annexer une information
d'identification de noeud (204a) au mot de passe
de réseau (254), avant l'étape de communication
du mot de passe de réseau (254) au serveur de ré-
seau (201).

20. Le système d'ordinateur (S) de la revendication 15,
dans lequel le jeton externe (188) est une carte à
microprocesseur.

21. Le système d'ordinateur (S) de la revendication 15,
dans lequel le jeton externe (188) est un dispositif
Touch Memory (marque déposée).

22. Le système d'ordinateur (S) selon la revendication
15, dans lequel la clé de chiffrement (256) est uni-
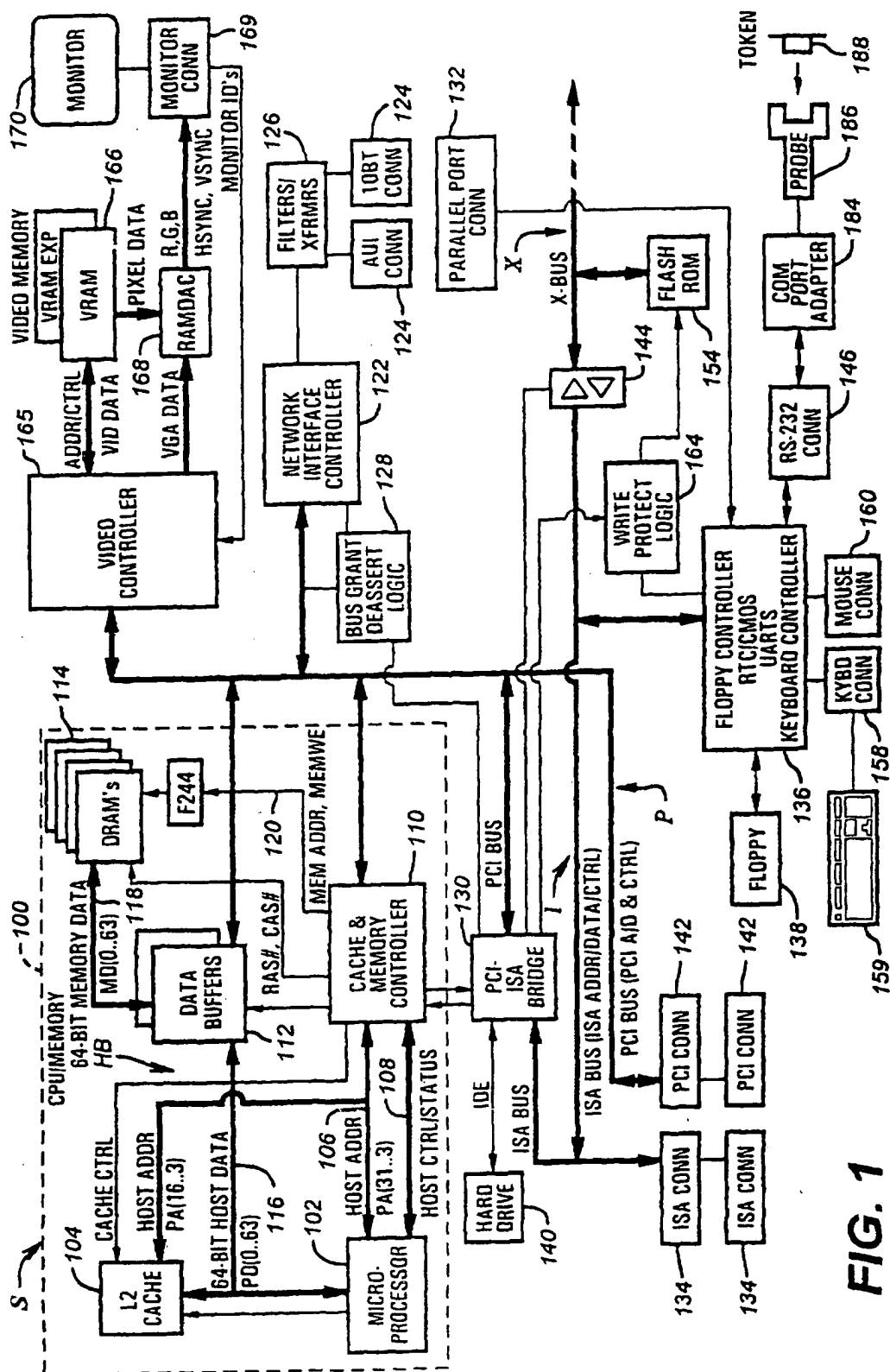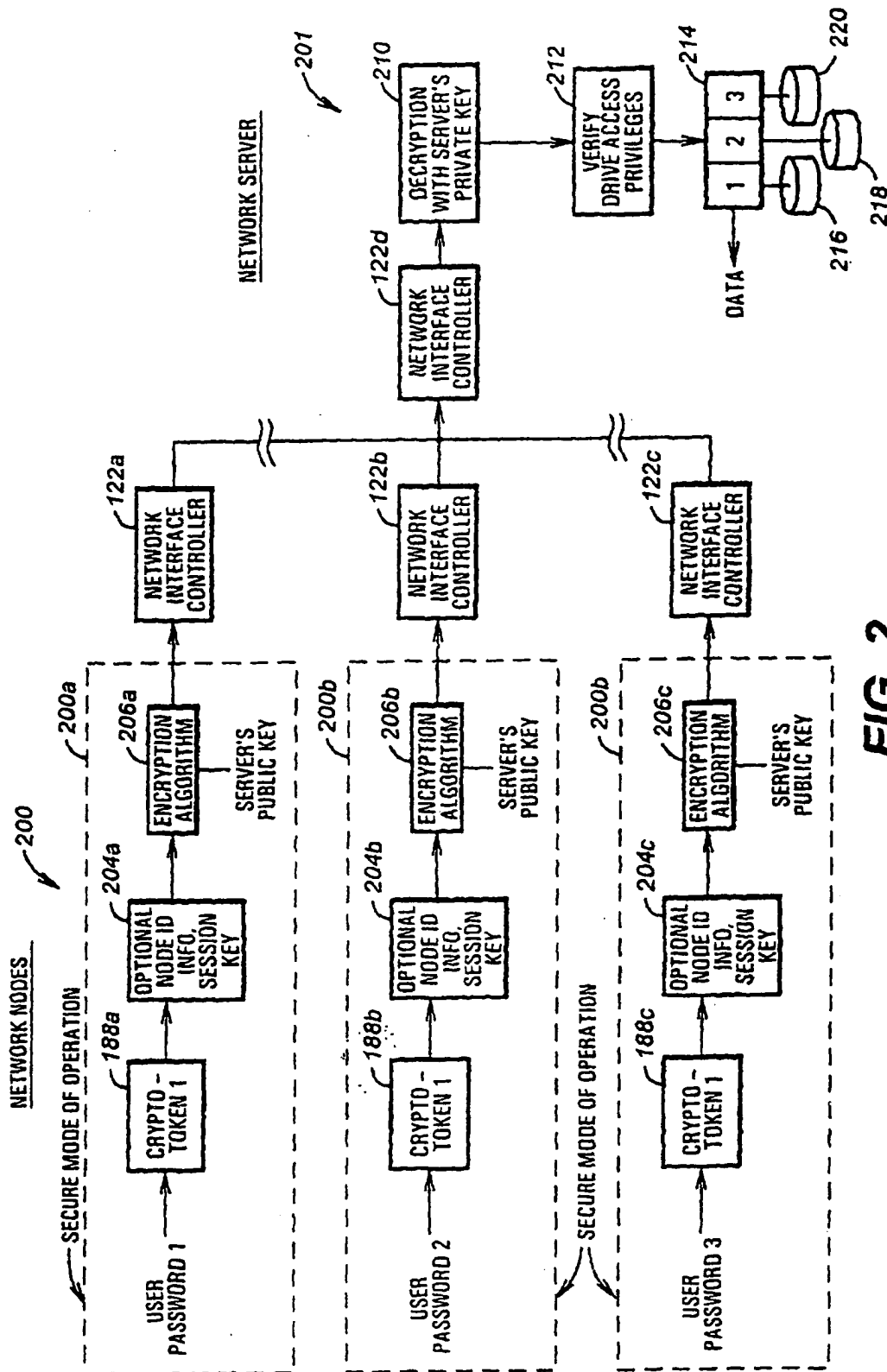que ou produite en quantité limitée.

FIG. 1

BEST AVAILABLE COPY
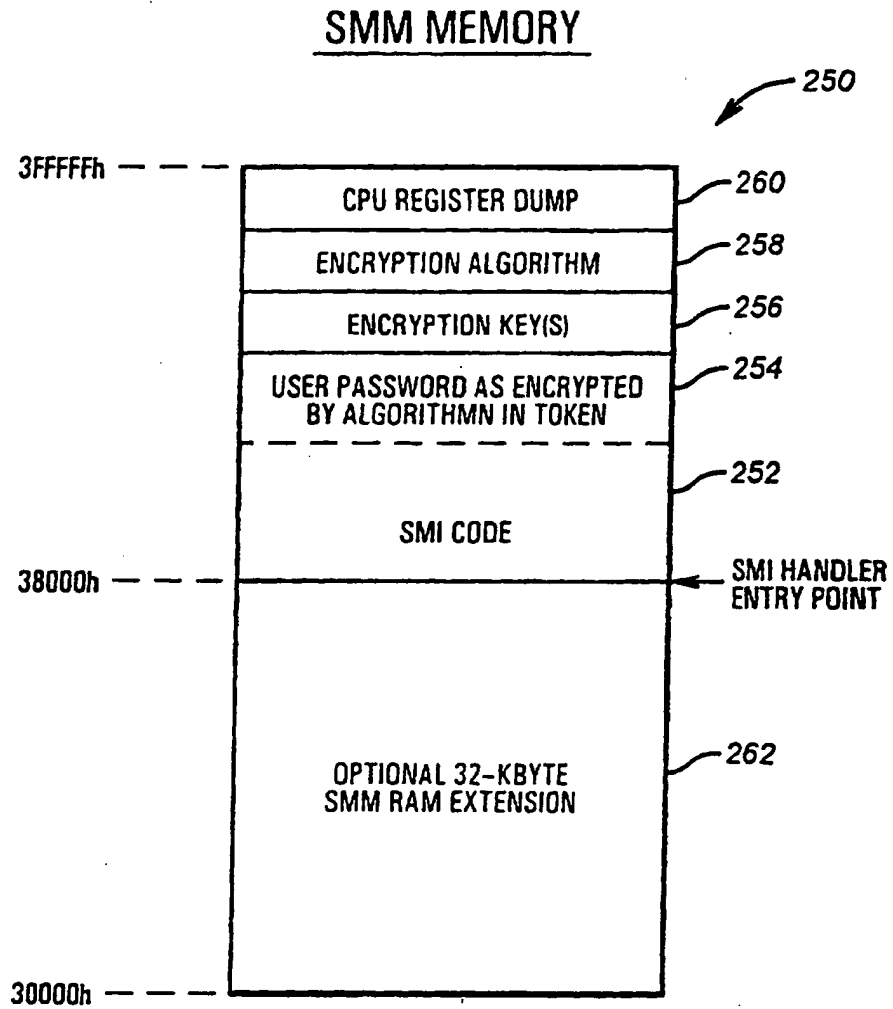
FIG. 2

BEST AVAILABLE COPY

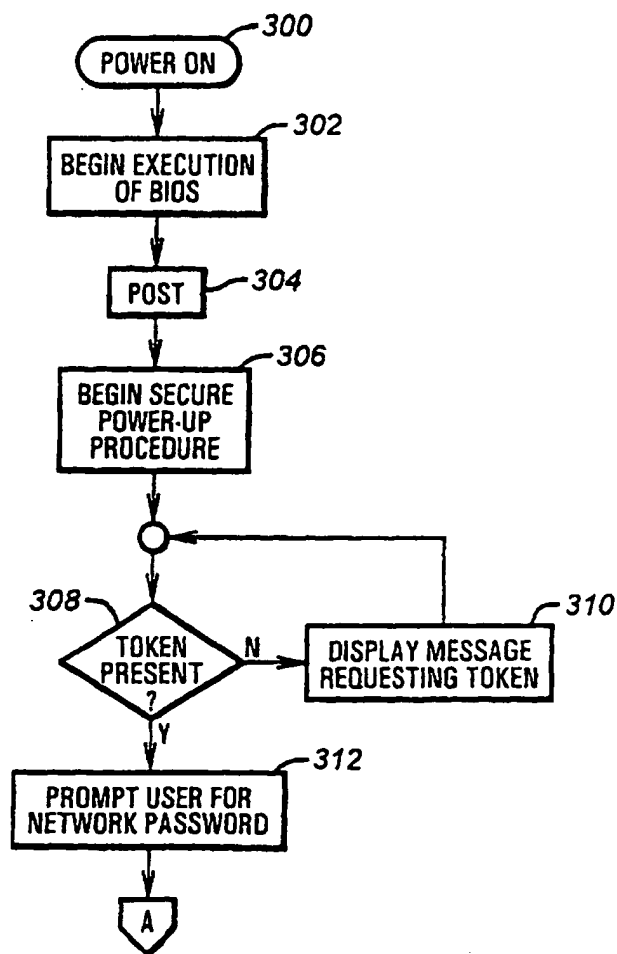## SMM MEMORY

250

3FFFFFh ——— —

CPU REGISTER DUMP	260
ENCRYPTION ALGORITHM	258
ENCRYPTION KEY(S)	256
USER PASSWORD AS ENCRYPTED BY ALGORITHMN IN TOKEN	254

252

SMI CODE

38000h ——— —

← SMI HANDLER
ENTRY POINT

262

OPTIONAL 32-KBYTE
SMM RAM EXTENSION

30000h ——— —

FIG. 3

POWER ON — 300

BEGIN EXECUTION
OF BIOS — 302

POST — 304

BEGIN SECURE
POWER-UP
PROCEDURE — 306

308 — TOKEN
PRESENT
?

N → DISPLAY MESSAGE
REQUESTING TOKEN — 310

Y

PROMPT USER FOR
NETWORK PASSWORD — 312

A

FIG. 4A

A

ENCRYPT PASSWORD
USING ENCRYPTION
ALGORITHM IN TOKEN — 314

APPEND OPTIONAL
NODE IDENTIFICATION
INFORMATION — 316

ENCRYPT PERHIPHERAL
PASSWORD USING
ENCRYPTION ALGORITHM
IN TOKEN — 318

CONTINUE SECURE
POWER-UP PROCEDURE — 320

FIG. 4B